T-79.5501 Cryptology
Homework 2
September 29&30, 2005

1. The keystream z_i, $i = 1, 2, \ldots$ of a binary stream cipher is generated by repeating a finite random sequence $K = (k_1, \ldots, k_m)$ of m bits, which is the key. Hence $z_i = k_i$, for $i = 1, 2, \ldots, m$, and $z_{i+m} = z_i$, for all $i = 1, 2, \ldots$.

   a) This stream cipher is used to encrypt plaintext with redundancy R_L. Give an estimate for the unicity distance.

   b) Suppose that $m = 5$ and the plaintext bit string is formed by repeating the following procedure (a finite number of times): two bits are generated at random, and a third bit is computed as an xor sum of these two bits. The first fifteen bits of the ciphertext are: 0 1 0 1 0 1 1 1 1 1 0 0 0 0 1. Attempt to find the key $K = (k_1, k_2, k_3, k_4, k_5)$.

2. The DES keys are 64 bits long, where each eighth bit is a parity bit computed as a modulo 2 sum of the preceding seven bits. A key management center uses DES encryption algorithm and a "master" DES key to encrypt DES keys to end users. Each ciphertext block consists of one encrypted DES key. Estimate the unicity distance of this cryptosystem, that is, estimate the number of encrypted end users' DES keys that an attacker needs to uniquely compute the master key given enough computing time.

3. (Garbage in between) Consider a cryptosystem where $|\mathcal{P}| = |\mathcal{C}|$ and keys are chosen equiprobably. This cryptosystem is used to encrypt language L, which consists of strings of plaintext characters and has entropy H_L, redundancy R_L and unicity distance n_0. The language L is modified in such a way that after each block of d characters s plaintext letters are chosen uniformly random from $\mathcal{P}$ and inserted to the plaintext. What is the entropy, redundancy and the unicity distance of the modified language?

4. Compute $\gcd(9211, 4880)$, and find integers s and t such that $9211s + 4880t = \gcd(9211, 4880)$.

5. Solve the following congruence equations and systems.

   a)
   $$5x \equiv 4 \pmod{668}$$

   b)
   $$15x \equiv 12 \pmod{2004}$$

   c)
   $$\begin{aligned} 15x &\equiv 12 \pmod{2004} \\ 11x &\equiv 5 \pmod{2005} \end{aligned}$$